KRYPTOGRAFIE
KRYPTOANALÝZA
STEGANOGRAFIE

CO TO JE - KRYPTOGRAFIE

Věda o šifrování informací. Šifrování je proces přeměny dat do tajné podoby, tzv. šifry. Šifra je text, který bez znalosti klíče vypadá nesrozumitelně. K dešifrování šifry a získání zpět původních dat se používá dešifrovací klíč.

Kryptografie se používá v mnoha oblastech například

Ochrana dat v počítačích a na internetu
Bezpečná komunikace (například e-mail)
Elektronický podpis
Ochrana licencí softwaru

CO TO JE - KRYPTOANALÝZA

Kryptoanalýza je věda o prolamování šifer. Kryptoanalytici se snaží najít způsoby, jak dešifrovat šifry bez znalosti dešifrovacího klíče.

Existuje mnoho technik kryptoanalýzy, a to jak matematických, tak statistických. Kryptoanalytici používají tyto techniky k nalezení slabin v šifrách a k jejich prolomení.

Kryptoanalýza hraje důležitou roli v kryptografii. Pomáhá kryptografům navrhovat silnější šifry, které odolávají známým technikám kryptoanalýzy

CO TO JE - **STEGANOGRAFIE**

Steganografie je věda o ukrývání informací do jiných dat. Cílem steganografie je skrýt existenci tajné zprávy tak, aby nebyla na první pohled patrná.

Existuje mnoho technik steganografie, a to jak analogových, tak digitálních. Analogové techniky steganografie zahrnují například ukrývání zpráv do neviditelného inkoustu nebo do mikroteček. Digitální techniky steganografie zahrnují například ukrývání zpráv do obrázků, zvukových souborů nebo video souborů.

Šifry

Symetrické

Symetrické šifry používají pro šifrování i dešifrování stejný klíč. To znamená, že ten, kdo chce zprávu zašifrovat, musí klíč sdílet s příjemcem. Pokud by se klíč dostal do nesprávných rukou, mohl by ho někdo použít k dešifrování zprávy a zneužití informací.

Symetrické šifry jsou obvykle velmi rychlé a efektivní. To je důležité pro šifrování velkých objemů dat.

Asymetrické

Asymetrické šifry používají dva klíče: šifrovací a dešifrovací. Šifrovací klíč je veřejný a může ho znát kdokoli. Dešifrovací klíč je tajný a zná ho pouze příjemce zprávy.

To umožňuje bezpečné sdílení informací s lidmi, které neznáme. Můžeme jim poslat zprávu zašifrovanou jejich veřejným klíčem a oni ji budou moci dešifrovat pouze svým tajným klíčem.

Asymetrické šifry jsou obvykle pomalejší než symetrické šifry. To je způsobeno složitější matematikou, která je pro jejich fungování nutná.

HASHOVACÍ FUNKCE

Hashovací funkce

Hashovací funkce je matematická funkce, která převádí libovolné množství dat na pevnou délku výstupu, tzv. hash. Hash je jedinečný identifikátor dat a lze ho použít k jejich ověření.

Jak to funguje?

Hashovací funkce zpracovává data po blocích a z každého bloku vypočítá dílčí hash. Dílčí hashe se pak kombinují do finálního hashe. Změna i jediného bitu v datech způsobí změnu finálního hashe.

Příklady hashovacích funkcí

MD5

Jedná se o starší hashovací funkci, která není tak bezpečná jako novější funkce.

SHA-1

Jedná se o rozšířenější hashovací funkci, která je stále považována za bezpečnou pro většinu aplikací.

SHA-2

Jedná se o novější a bezpečnější hashovací funkci, která je dostupná ve více variantách (SHA-224, SHA-256, SHA-384 a SHA-512).

SUBSTITUČNÍ – ŠIFRY

Jsou typem šifry, která nahrazuje jednotlivé znaky v textu jinými znaky. Existuje mnoho druhů substitučních šifer.

Představme si, že chceme zašifrovat text "Ahoj světe!" pomocí jednoduché substituční šifry, kde každý znak je nahrazen znakem o 3 pozice dále v abecedě. Šifrovací tabulka pro tuto šifru by vypadala takto:

A -> D	**X -> Z**
B -> E	**Y -> A**
C -> F	**Z -> B**

Původní text: "Ahoj světe!"
Šifrovací tabulka: A->D, B->E, C->F, ...
Zašifrovaný text: "Dkrj vžwhh!"

TRANSPOZIČNÍ – ŠIFRY

Na rozdíl od substitučních šifer, nemění samotné znaky v textu, ale pouze jejich pořadí. Tyto šifry operují s přeskupováním písmen podle předem stanoveného pravidla.

Příklady transpozičních šifer

Šifra psaná pozpátku
Nejjednodušší příklad, kdy se písmena v textu pouze otočí opačně.

Původní text: "ABECEDA„
Zašifrovaný text: "ADEBCBA"

Transpozice řádků
Text se rozdělí na řádky a ty se následně přehodí podle daného pravidla.
Původní text: "Ahoj světe!„
Šifrovací pravidlo: 2. řádek -> 1. řádek, 1. řádek -> 3. řádek
Zašifrovaný text: "te! Ahoj svě"

DIGITÁLNÍ PODPIS.

Je elektronická forma podpisu, která slouží k ověření identity odesílatele a integrity zprávy. Jedná se o soubor dat, který je generován kryptografickými metodami a je připojen k digitální zprávě. Digitální podpis umožňuje příjemci zprávy:

Princip fungování

Digitální podpis se vytváří pomocí kryptografické funkce, která generuje dva klíče:

Soukromý klíč: Klíč, který je znám pouze odesílateli a slouží k vytváření podpisu.

Veřejný klíč: Klíč, který je dostupný všem a slouží k ověření podpisu.

Odesílatel zprávy vygeneruje digitální podpis pomocí svého soukromého klíče a připojí ho k odesílané zprávě. Příjemce zprávy pak ověří podpis pomocí veřejného klíče odesílatele. Pokud je podpis platný, příjemce má jistotu, že zpráva pochází od dané osoby a že nebyla po odeslání změněna.

DĚKUJI ZA POZORNOST

Vojtěch Pinkas 4.TA